



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,622	03/30/2004	Kazumasa Omote	1924.70199	3471
<div>7590 05/11/2007</div> <div>Patrick G. Burns, Esq. GREER, BURNS & CRAIN, LTD. Suite 2500 300 South Wacker Dr. Chicago, IL 60606</div>				
<div>EXAMINER</div> <div>JOHNSON, CARLTON</div>				
<div>ART UNIT PAPER NUMBER</div> <div>2136</div>				
<div>MAIL DATE DELIVERY MODE</div> <div>05/11/2007 PAPER</div>				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/812,622	Applicant(s) OMOTE ET AL.	
	Examiner Carlton V. Johnson	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>3-30-2004/4-20-2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responding to application papers filed on **3-20-2004**.
2. Claims **1 - 20** are pending. Claims **1, 12, 13, 14** are independent.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim **1 - 20** are rejected under 35 U.S.C. 102(e) as being anticipated by **Spiegel et al.** (US Patent No. **7,159,149**).

Regarding Claims 1, 13, 14, Spiegel discloses a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, causes a computer to perform:

- a) acquiring information related to a traffic and a communication address of a communication packet based on setting information; (see Spiegel col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means; col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and

destination addresses and information not matching criteria for normal traffic setting) and

- b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria. (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

Regarding Claims 2, 15, Spiegel discloses the computer program, device according to claims 1, 14, causes the computer to further perform changing the setting information upon it is judged at the judging that the communication is executed by the worm, wherein the acquiring includes acquiring the information based on the setting information after change. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters for worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claims 3, 16, Spiegel discloses the computer program, device according to claims 1, 14, causes the computer to further perform changing the judgment criteria upon it is judged at the judging that the communication is executed by the worm, wherein the judging includes judging whether the communication is executed by the worm based on the information acquired and the setting information after change. (see Spiegel col. 5, lines 8-10; col. 5, lines 15-21: worm determination based on information and adjusted (i.e. changed) information; col. 6, lines 15-22: software, implementation

means)

Regarding Claims 4, 17, Spiegel discloses the computer program, device according to claims 1, 14, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: network communication packets throughput increased, worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claims 5, 18, Spiegel discloses the computer program, device according to claim 4, 17, wherein the judging includes judging that a communication from a plurality of computer in the predetermined segment is executed by the worm when

- a) a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored; col. 6, lines 15-22: software, implementation means) and
- b) the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet

acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: worm determination based on number of packets transferred to addresses (i.e. inside or outside local network))

Regarding Claims 6, 19, Spiegel discloses the computer program, device according claims 1, 14, wherein the judging includes judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when

- a) there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, (see Spiegel col. 4, lines 17-22: communications increase (i.e. inside or outside local network), worm determination; col. 6, lines 15-22: software, implementation means) and
- b) there is an increase in number of sender addresses of the communication packets. (see Spiegel col. 3, lines 20-27: communications (i.e. address, and process port number) increases, worm determination)

Regarding Claims 7, 20, Spiegel discloses the computer program, device according to claims 1, 14, wherein the judging includes outputting any one of information about a computer that performed the communication and a communication status upon it is judged that the communication is executed by the worm. (see Spiegel col. 3, lines 58-

63; col. 4, lines 11-16: source address (i.e. for a computer) a factor in worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 8, Spiegel discloses the computer program according to claim 1, wherein the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 9, Spiegel discloses the computer program according to claim 1, causes the computer to perform cutting off the communication executed by the worm upon it is judged that the communication is executed by the worm. (see Spiegel col. 2, lines 13-18: terminate network access (i.e. cut off communications), worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 10, Spiegel discloses the computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by stopping a process that is started by the worm. (see Spiegel col. 2, lines 13-18: terminate affected process (i.e. stopping a process), worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 11, Spiegel discloses the computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have a worm. (see Spiegel col. 6, lines 48-55: firewall functioning; col. 6, lines 15-22: software, implementation means)

Regarding Claim 12, Spiegel discloses the computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

- a) acquiring information related to a traffic and a communication address of a communication packet based on setting information; (see Spiegel col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means; col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses) and
- b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria. (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications based on worm, threshold criteria)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



CVJ
May 4, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


5,9107

Carlton V. Johnson
Examiner
Art Unit 2136